

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of

)	
)	
Protecting Against National Security)	ET Docket No. 21-232
Threats to the Communications Supply)	
Chain through the Equipment)	
Authorization Program)	
)	
Protecting Against National Security)	ET Docket No. 21-233
Threats to the Communications Supply)	
Chain through the Competitive Bidding)	
Program)	

Comments of Hytera U.S.

Marjorie K. Conner
Its Counsel
mkconner@mkconnerlaw.com
703-626-6980

September 17, 2021

Table of Contents

<i>Summary</i>	i
1. Hytera	2
2. Protection of the U.S. Communications and Equipment Supply Chain	4
<i>a. Confusion arising from Conflation</i>	4
<i>b. Section 1601 Limits the FCC’s Authority to Regulation of “Covered Equipment.”</i>	7
<i>c. Section 1601 Delegates Authority to Determine Covered Equipment</i>	7
<i>d. Absent an Authoritative Designation, the Commission May Not Extend its Proposed Rules Beyond Covered Equipment to Cover Entities on the Covered List</i>	8
<i>e. The Commission’s Proposed Rules Should be Limited to Covered Equipment</i>	9
3. The Commission Should Clarify the Scope of the Covered List	9
<i>a. The Commission Should Publish its Definition of Covered Equipment in the Publication of the Covered List</i>	9
<i>b. The Commission Should Publish the Use and Capability Qualifications in the Publication of the Covered List.</i>	10
<i>i. The Use Qualification</i>	10
<i>ii. The Capability Qualification</i>	10
<i>iii. The Commission’s Website Should be Updated</i>	11
4. Proposed Rule Amendments	11
<i>a. Section 2.911(d)(5)</i>	12
<i>b. U.S. Based Responsible Party</i>	13
<i>c. The Proposed Revisions to Section 2.906 of the Commission’s Rules: The Supplier’s Declaration of Conformity (“SDoC”) Exceed the Scope of Section 1601 Act</i>	13
<i>d. Proposed Revisions to Section 2.907: The Complement to Section 2.906</i>	14
5. Enforcement Policies	14
<i>a. Revocation of Existing Authorizations</i>	15
<i>b. Enforcement Reliance on Public Reports</i>	15
6. The Commission May Not Exceed the Authority Granted by Congress	17

Summary

Hytera U.S., Inc. by counsel, and in response to the Notice of Proposed Rule Making and Notice of Inquiry (“NPRM”) issued by the Federal Communications Commission (“FCC” or “Commission”) on June 17, 2021, in the captioned proceeding, submits these comments on the Commission’s proposed rules concerning identification and regulation of communications equipment and services included on the Covered List first created by the 2019 NDAA,¹ and included at Section 1601 – 1609 of the Communications Act of 1934, as amended, 47 U.S.C. §§1601-1609 (the “Act”), by the Secure Networks Act.²

Hytera U.S. supports the Commission’s efforts to ferret out unsecure equipment from our nation’s critical communications infrastructure. Hytera notes that the Commission’s authority is strictly limited by Section 1601 of the Act. But confusion reigns over those limits. Flyers distributed by competitors, press reports, and even Commissioner Carr’s separate statement accompanying the NPRM conflate the entities listed with the effect of the Covered List.

Hytera US’ dealers have suffered greatly, losing deals, being barred from bidding for projects, being maligned, generally – all based on conflation of the entities on the list with effect of the Covered List.³ This suffering is largely competitor-sponsored. But industry press has perpetuated the conflation. On June 16, 2021, Bloomberg reported that U.S. regulators proposed

¹ Section 889(f)(3) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 132 Stat. 1918).

² Secure and Trusted Networks Act of 2019, Pub. Law 116-124, 134 Stat. 158 (2020) (“Secure Networks Act”).

³ See MicroMagic Co. Inc. Comments, filed August 24, 2021; East Mountain Communications Comments filed August 24, 2021; Communications Associates Comments, filed August 26, 2021; Diversified Communications Group Comments, filed September 7, 2021; Baker’s Communications, Inc., and Warner Communications, both filed with Hytera’s *ex parte* notice filed August 17, 2021 (collectively, “Hytera Dealer Letters”). All these local dealers report business lost to false assertions that Hytera’s *LMR/DMR equipment* is on the Covered List. Collectively attached as Attachment 6.

a ban on products from two-way radio maker HCC.⁴ The Bloomberg article noted that the FCC said it may also revoke its previous authorizations for equipment from the companies, conflating the entities on the Covered List with the actual communications equipment and services on the Covered List.

More recently, *Broadband Breakfast* published a report about a filing in this proceeding. The report accurately noted the commenter's objections to Hytera's inclusion on the Covered List. It went on to conflate entities with the Covered List. "In March, the FCC announced that it had designated Hytera among other Chinese businesses with alleged links to the Communist government."⁵

To the extent the Commission has authority to adopt and enforce the rules and policies proposed in this proceeding, that authority is limited by the definition of "communications equipment and services" which the Commission, itself adopted in the *Supply Chain Second Report and Order*,⁶ as "any equipment or service used in fixed and mobile networks that provides advanced communication service, provided the equipment or service uses electronic components."⁷ The Commission went on to interpret "advanced communication service" to mean high-speed, switched, broadband telecommunications capability that enables users to originate quality voice, data, graphics, and video telecommunications using any technology with connection speed of at least 200 kbps in either direction.⁸

⁴ Shields, Todd, *FCC Proposes Ban on Chinese Surveillance Cameras, Other Products*, Bloomberg, June 16, 2021, <https://www.bloomberg.com/news/articles/2021-06-17/chinese-surveillance-cameras-targeted-by-fcc-on-security-worries> (Accessed September 14, 2021). Attachment 7.

⁵ Hathout, Ahmad, *Hytera's Inclusion on FCC's National Security Blacklist 'Absurd, Client Says*, Broadband Breakfast, September 8, 2021, <https://broadbandbreakfast.com/2021/09/hyteras-inclusion-on-fccs-national-security-blacklist-absurd-client-says/> (accessed September 17, 2021). Attachment 8.

⁶ *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Second Report and Order, 35 FCC Rcd 14824, 14301 (2020) ("Supply Chain Second Report and Order").

⁷ NPRM at para. 17.

⁸ *Id.*

Before communications equipment and services may be included on the Covered List, not only must it be used to provide advanced communication services at a connection speed of at least 200 kbps in either direction, the equipment must also meet the Use Qualification and the Capability Qualification, both included in Section 1601 of the Act. If the communications equipment and services do not meet the technical definition adopted by the Commission in the *Supply Chain Second Report and Order*, or either of the Use Qualification or the Capability Qualification, set forth in the Act, the communications equipment and services are not on the Covered List – they are not Covered Equipment.

This confusion is almost understandable. Commissioner Carr, in his separate statement to the NPRM stated that the FCC’s actions in the *Supply Chain Second Report and Order* “established the FCC’s Covered list to designate *entities* that pose an unacceptable risk to our national security.”⁹ (Emphasis added.)

Of course, this is not true. The Covered List relates to communications equipment and services that pose an unacceptable risk to U.S. national security, as defined in the *Supply Chain Second Report and Order* and Section 1601 of the Act.

Hytera asks that the Commission set the record straight. To do this, the Commission must expressly define Covered Equipment on its webpage devoted to the Covered List, including the technical definition, the Use Qualification, and the Capability Qualification, and that it limit the applicability of its rules to Covered Equipment so defined.

Hytera also asks that the Commission add attestations specific to the character and capabilities of the equipment proposed for certification to the certification required under Section 2.911(d)(5) of the Commission’s rules. These attestations will require the applicant to consider the character and capabilities of the equipment proposed for certification and to certify under penalty of perjury that the equipment is not on the Covered List.

⁹ NPRM at p. 59. *Cf.* 35 FCC Rcd 14824, 1430.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of

)	
)	
Protecting Against National Security)	ET Docket No. 21-232
Threats to the Communications Supply)	
Chain through the Equipment)	
Authorization Program)	
)	
Protecting Against National Security)	ET Docket No. 21-233
Threats to the Communications Supply)	
Chain through the Competitive Bidding)	
Program)	

Comments of Hytera U.S.

Hytera U.S. Inc. (“Hytera U.S.”), by counsel, and in response to the Notice of Proposed Rule Making and Notice of Inquiry (“NPRM”) issued by the Federal Communications Commission (“FCC” or “Commission”) on June 17, 2021, in the captioned proceeding, comments on the actions proposed. Hytera is pleased to share its experience with the Commission in this proceeding. Hytera endorses the Commission’s careful approach to defining the reach of its proposed rules and urges the Commission to adopt rules to help more clearly define the scope of the communications equipment and services identified in Section 1601(c) of the Communications Act of 1934, as amended (the “Act”), 47 U.S.C. §1601(c) (“Covered Equipment”) and is listed in Section 1601(c) of the Act (“Covered List”).¹

¹ Sections 1601-1609 of the Communications Act of 1934, as amended, 47 U.S.C. §§1601-1609, were adopted in the Secure and Trusted Networks Act of 2019, Pub. Law 116-124, 134 Stat. 158 (2020) (“Secure Networks Act”).

1. Hytera

Hytera U.S. Inc. is a U.S. corporation, organized under the laws of the state Delaware, and authorized to do business in the states of California and Florida.² Hytera U.S. has offices in Sunrise, Florida, and Irvine, California. In the U.S., Hytera U.S. markets HCC manufactured products through hundreds of local, U.S.-based independent dealers throughout the U.S. In contrast to other manufacturers, Hytera dealers are generally small family-owned small businesses.³ Hytera U.S. gives back to its communities, including working with its local dealers to support COVID-19 response. For example, in partnership with Abest Communications, Hytera provided radios to Hatzalah Emergency Services in New York to aid in the fight against COVID-19.⁴ In partnership with its local dealer, Alpha Prime Communications, Hytera donated radios to Northwestern Medicine Lake Forest Hospital to assist in resource coordination in response to COVID-19.⁵ In partnership with Warner Communications, the local dealer in St. Louis, Missouri, Hytera donated radios to Mercy Hospital St. Louis to help provide testing and save lives during the COVID-19 pandemic.⁶ Additionally, Hytera provided radios to the annual caravan run by Wreaths Across America to deliver wreaths to Arlington National Cemetery.⁷

² Hytera US acquired Hytera Communications America (East) and Hytera Communications America (West) through a bankruptcy proceeding, *In re HCA West*, No. 8:20-bk-11507, (*Order (1) Approving Purchase Agreement Among the Debtors and the Purchaser, (2) Approving Sale of the Inventory of the Debtors Free and Clear of All Liens, Claims, Encumbrances and Other Interests Pursuant to Bankruptcy Code Sections 105, 363(b), (f), and (m), and Granting Related Relief*) (Bankr.C.D.Cal. May 10, 2021)

³ As the U.S. marketing arm of the company, Hytera U.S. has a direct interest in the development of the rules under consideration in this proceeding. Hytera U.S. supports HCC's comments, and, to the extent they are different from Hytera U.S.' comments, adopts them in full.

⁴ <https://www.hytera.us/news/hytera-america-donates-radios-to-hatzalah-emergency-services-to-fight-the-covid-19-pandemic-in-new-york> (Accessed September 17, 2021), Attachment 1.

⁵ <https://www.hytera.us/news/hytera-america-donates-radios-to-northwestern-medicine-lake-forest-hospital> (Accessed September 17, 2021), Attachment 2.

⁶ <https://www.hytera.us/news/hytera-america-donates-radios-to-mercy-to-fight-the-covid-19-pandemic-in-st-louis> (Accessed September 17, 2021), Attachment 3.

⁷ <https://www.hytera.us/news/hytera-provides-push-to-talk-over-cellular-communications-to-wreaths-across-america> (Accessed September 17, 2021), Attachment 4.

Hytera U.S. is wholly owned by Hytera Communications Co. Ltd. (“HCC”), a publicly traded, independently managed corporation that offers consumer products for civilian and commercial use. HCC is organized under the laws of China and listed on the Shenzhen Stock Exchange. More than fifty-two percent (52%) of the voting rights in HCC are held under a weighted voting rights structure by co-founders Chen Qingzhou and Weng Limin. HCC is not owned or controlled by or otherwise affiliated with the Chinese government; it is not owned or controlled by any entity affiliated with the Chinese defense industrial base. HCC has no ties to the Chinese Communist Party.

HCC has ten (10) international research and development (“R&D”) Innovation Centers and more than ninety (90) regional organizations around the world, including in Canada, Germany, and Spain. Worldwide Hytera employs over 6,800 people worldwide and more than forty percent (40%) of HCC’s employees are engaged in engineering, research, and product design.⁸

HCC makes handsets, repeaters, and trunking systems. HCC develops and markets wireless two-way radios and private systems tailored to its customers’ needs. Hytera’s customers hold their own licenses to operate the stations using Hytera equipment.⁹ Hytera’s equipment is designed for use on spectrum licensed under Part 90 of the FCC’s rules.

End users of Hytera equipment are generally smaller businesses in a range of sectors, including government, local public utilities, taxi companies, delivery services, towing companies, hotels, restaurants, large department stores, and schools and universities. The

⁸ Qian, Zhang, “*Innovation Keeps Hytera at Global Forefront: Founder*,” *Shenzhen Daily*, October 31, 2018, https://www.eyeshenzhen.com/content/2018-10/31/content_21183908.htm (Accessed September 17, 2021). Attachment 5.

⁹ Hytera U.S. holds a single FCC license, WQZW796, for temporary operations on a secondary basis. Hytera’s technicians use the licensed facilities for testing and duplicating reported issues with equipment, so that they may develop solutions.

imprecise language used in the Covered List and reflected in the proposed rules has negatively impacted these Hytera's end users and, even more, Hytera's independent dealer network.¹⁰ The vague wording of the Covered List on the FCC's website has led to the spread of misinformation in the marketplace about what is Covered Equipment. This proceeding gives the Commission the opportunity to publish the precise definition of Covered Equipment, as set forth in Section 1601 of the Act and as the Commission published in the *Supply Chain Second Report and Order*.¹¹

2. Protection of the U.S. Communications and Equipment Supply Chain

In this proceeding, the Commission proposes rules related to equipment authorization and its competitive bidding procedures more certainly to secure our nation's critical communications networks. While tightening its restrictions on the communications equipment and services authorization and certification process, the Commission must take care to provide clear guidance with precise rules, in accord with its authority. Particularly, with respect to this proceeding, the Commission's authority is specifically limited by Section 1601 of the Act.¹²

a. Confusion arising from Conflation

Competitors, trade press, and even Commissioner Carr have conflated the actual extent of the Covered List to aver that it covers the entities that manufacture the communications

¹⁰ See MicroMagic Co. Inc. Comments, filed August 24, 2021; East Mountain Communications Comments filed August 26, 2021; Communications Associates Comments, filed August 27, 2021; Diversified Communications Group Comments, filed September 8, 2021; FreCom Inc. Comments, filed September 14, 2021; GSEAC, Inc. Comments, filed September 11, 2021; MetroTalk Comments, filed September 13, 2021; Alpha Prime Communications Comments, filed September 14, 2021; Voceon Digital Radio Communications Comments, filed September 15, 2021; Baker's Communications, Inc., and Warner Communications, both filed with Hytera's *ex parte* notice filed August 17, 2021 (collectively, "Hytera Dealer Letters"). All these local dealers report business lost to false assertions that Hytera's *LMR/DMR equipment* is on the Covered List. Attachment 6.

¹¹ *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Second Report and Order, 35 FCC Rcd 14824, 14301 (2020) ("*Supply Chain Second Report and Order*").

¹² The Commission adopted rules to discharge its duties under the Secure Networks Act. See Subpart DD of the Commission's rules, 47 C.F.R. 1.50001-1.50007, including the Appendices.

equipment and provide the services that might be listed on the Covered List (the “Covered Equipment”). Competitors distribute flyers and trade press articles to assert that any equipment made by any of the entities listed on the Covered List are unsecure; buyers of any equipment made by any of the entities on the Covered List will be required to remove and replace that equipment, perhaps at their own cost. Of course, that is not true.

In the *Supply Chain Second Report and Order*, the Commission clearly limited the effect of the Covered List to Covered Equipment, consistent with Section 1601 of the Act. It said, “rather than the proposed blanket prohibition to all equipment and services produced by a manufacturer, ...[t]he Covered List is limited to such equipment and services that the federal government, including the U.S. intelligence community, has identified as national security threats and that are placed at the most vulnerable spots in our communications infrastructure.”¹³

Despite this clear statement, confusion persists. Hytera’s competitors have used the confusion to their advantage, and industry press has perpetuated the conflation. On June 16, 2021, Bloomberg reported that U.S. regulators proposed a ban on products from two-way radio maker HCC.¹⁴ The Bloomberg article noted that the FCC said it may also revoke its previous authorizations for equipment from the companies, conflating the entities on the Covered List with the actual communications equipment and services on the Covered List.

More recently, *Broadband Breakfast* published a report about a filing in this proceeding. The report accurately noted the commenter’s objections to Hytera’s inclusion on the Covered List. It went on to conflate entities with the Covered List. “In March, the FCC announced that it

¹³ 35 FCC Rcd 14824, 14301.

¹⁴ Shields, Todd, *FCC Proposes Ban on Chinese Surveillance Cameras, Other Products*, Bloomberg, June 16, 2021, <https://www.bloomberg.com/news/articles/2021-06-17/chinese-surveillance-cameras-targeted-by-fcc-on-security-worries> (Accessed September 14, 2021). Attachment 7.

had designated Hytera among other Chinese businesses with alleged links to the Communist government.”¹⁵

No wonder there is confusion. In his separate statement accompanying the NPRM, in citing the actions in the *Supply Chain Second Report and Order*, Commissioner Carr said, the FCC “established the FCC’s Covered List to designate *entities* that pose an unacceptable risk to our national security.”¹⁶ (Emphasis added.) In contrast, the Commission, in the *Supply Chain Second Report and Order*, actually rejected applying the Covered List to entities.

This proceeding presents an opportunity for the Commission to clearly define the reach of the Covered List. The Commission may revised the publication on the FCC website to state that the Covered List is limited by the definition of “communications equipment and services” which the Commission, itself defined in the *Supply Chain Second Report and Order*,¹⁷ as “any equipment or service used in fixed and mobile networks that provides advanced communication service,¹⁸ provided the equipment or service uses electronic components.”¹⁹ The Commission should also include its definition of “advanced communications service” to mean high-speed, switched, broadband telecommunications capability that enables users to originate quality voice, data, graphics, and video telecommunications using any technology with connection speed of at

¹⁵ Hathout, Ahmad, “*Hytera’s Inclusion on FCC’s National Security Blacklist ‘Absurd,’*” Client Says, Broadband Breakfast, September 8, 2021, <https://broadbandbreakfast.com/2021/09/hyteras-inclusion-on-fccs-national-security-blacklist-absurd-client-says/> (accessed September 17, 2021). Attachment 8.

¹⁶ Carr Separate Statement, NPRM at 59.

¹⁷ 35 FCC Rcd 14824, 14301.

¹⁸ Section 1608(1) defines “advanced communication service” by reference to the definition of advanced telecommunications capability in section 1302 of the Act, which states: The term “advanced telecommunications capability” is defined, without regard to any transmission media or technology, as high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology.

¹⁹ NPRM at para. 17.

least 200 kbps in either direction.²⁰ This definition would be consistent with Section 1601 of the Act, so the Commission’s website may be updated without further formal action.

b. Section 1601 Limits the FCC’s Authority to Regulation of “Covered Equipment.”

Serious questions have been raised about the Commission’s authority to adopt and enforce the rules and policies proposed in this proceeding.²¹ If the Commission does have authority under current law, Section 1601 of the Act limits the Commission’s reach to Covered Equipment, and specifically does not reach the *entities* on the Covered List.

Applying the proposed rules only to the Covered Equipment is warranted by the Commission’s own words. In the *Supply Chain Second Report and Order*, the Commission specifically said, “[t]he Covered List is limited to such equipment and services that the federal government, including the U.S. intelligence community, has identified as national security threats and that are placed at the most vulnerable spots in our communications infrastructure.”²² Consistent with the interpretation in the *Supply Chain Second Report and Order*, in asking about its authority, in paragraph 67 in the NPRM, the Commission asked whether Section 302 of the Act provides an independent authority to deny equipment authorization to **equipment** deemed to pose an unacceptable security risk. (Emphasis added.) Even if the Commission wanted to expand the reach of the Covered List, it may not.

c. Section 1601 Delegates Authority to Determine Covered Equipment.

A close look at Section 1601 provides guidance on who has authority to determine which communication *equipment or service* poses an unacceptable risk to the national security of the

²⁰ *Id.*

²¹ Tatel, Jennifer B. and Clete D. Johnson, letter to Acting Chairwoman Jessica Rosenworcel, Commissioner Brendan Carr, Commissioner Geoffrey Starks, and Commissioner Nathan Simington, September 14, 2021. Attachment 9.

²² 35 FCC Rcd 14824, 14301.

United States or the security and safety of United States persons.²³ Any executive branch interagency body with appropriate national security expertise, including the Federal Acquisition Security Council established under Section 1322(a) of Title 41 of the U.S. Code may make a determination that communications equipment or service should be placed on the Covered List. The Department of Commerce may make such a specific determination pursuant to Executive Order No. 13873. A specific determination may be made by an appropriate national security agency, meaning the Department of Homeland Security, the Department of Defense, the Director of National Intelligence, the National Security Agency, or the Federal Bureau of Investigation.²⁴

Notably, FCC rule making proceedings are not listed as a means to expand the Covered List.²⁵

d. Absent an Authoritative Designation, the Commission May Not Extend its Proposed Rules Beyond Covered Equipment to Cover Entities on the Covered List.

With the Commission’s discretion as to which communications equipment and services limited by Section 1601 of the Act, the Commission may not, in this proceeding, extend its proposed rules to the *entities* listed in the Covered List, but must limit application of the new rules to Covered Equipment. The Commission expressly acknowledged in the *Supply Chain Second Report and Order* that a “more narrowly tailored rule instead supports a risk-based assessment of problematic equipment and services within a network, consistent with the approach taken in Section 889 of the 2019 NDAA²⁶ and ultimately incorporated into section 2 of

²³ 47 U.S.C. §1601(c).

²⁴ 47 U.S.C. §1608(2) of the Act for definition of Appropriate National Security Agency.

²⁵ In considering the limits on the Commission’s statutory authority, the *Chevron* framework first asks whether Congress has directly spoken to the precise question at issue. Section 1601(c) of the Act, in fact, does address the precise question at issue and delegates authority to offices and agencies other than the FCC. *See Huawei Techs USA, Inc. v. FCC*, 2 F 4th. 421, 433 (5th Cir. 2021), *citing Acosta v. Hensel Phelps Constr. Co.*, 909 F. 3d 723, 730 (5th Cir. 2018); *see also, Chevron U.S.A., Inc. v. Nat. Res. Def. Council, Inc.*, 467 U.S. 87, 842-44 (1984).

²⁶Section 889(f)(3) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 132 Stat. 1918).

the Secure Networks Act, rather than the proposed blanket prohibition to all equipment and services produced by a manufacturer.”²⁷

e. The Commission’s Proposed Rules Should be Limited to Covered Equipment.

The Commission may use the Covered List to ferret out insecure equipment on U.S. networks. Before it can begin, though, it must precisely define what Covered Equipment is. The definition must comply with the specific dictates of Section 1601 of the Act.

3. The Commission Should Clarify the Scope of the Covered List.

The NPRM seeks comment on the types of actions (e.g., outreach and education) that would be helpful to ensure that all parties potentially affected by the proposed rules understand the changes and will comply with the prohibition associated with Covered Equipment. Hytera urges the Commission to clarify the scope of the Covered List as set forth below so that all affected parties have clear and concise notice of exactly what is Covered Equipment, so that the anticompetitive distribution of false information about the Covered List may be effectively neutralized and purchasing decisions may be reliably made.

a. The Commission Should Publish its Definition of Covered Equipment in the Publication of the Covered List.

In the NPRM, the Commission cited the *Supply Chain Second Report & Order*,²⁸ to define communications equipment and service, as used in Section 1601 of the Act, to include any equipment or service used in fixed and mobile networks that provides advanced communication service, provided the equipment or service uses electronic components.²⁹ The Commission went on to interpret “advanced communications service” to mean high-speed, switched, broadband telecommunications capability that enables users to originate quality voice, data, graphics, and

²⁸ 35 FCC Rcd 14824 (2020).

²⁹ NPRM at para. 17.

video telecommunications using any technology with connection speed of at least 200 kbps in either direction.³⁰ However, this technical limitation is nowhere clearly and expressly stated on the Covered List on the Commission’s website; it is not clearly stated in the Public Notice of the publication of the Covered List. To ensure consistence with the Act, Hytera recommends that the Commission clarify that the Covered List only includes equipment and services providing broadband service having a connection speed of at least 200 kbps in either direction.

b. The Commission Should Publish the Use and Capability Qualifications in the Publication of the Covered List.

Further, Section 1601(b)(2) of the Act makes very clear that the communications equipment and services are not to be included on the Covered list unless they meet the specified Use Qualifications and Capability Qualifications.

i. The Use Qualification

The Use Qualification subjects video surveillance and telecommunications equipment provided or produced by Hytera Communication Corporation to the prohibitions of the Covered List only “to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes.”³¹

ii. The Capability Qualification

The Capability Qualification³² subjects video surveillance and telecommunications equipment provided or produced by Hytera Communication Corporation to the prohibitions of

³⁰ *Id.*

³¹ The Covered List incorporates wording from Section 1601(c)(3), which, in turn, is drawn Section 889(f)(3)(B) of the 2019 NDAA.

³² In Section 889(a)(2)(B) of the 2019 NDAA, this qualification was set forth as an exception to the applicability of the restrictions set forth in Section 889(a) of the 2019 NDAA. The recharacterization of the Capability Exception to a Capability Qualification indicates Congress’ focus on interconnected network equipment in its efforts to protect the nation’s communications supply chain.

the Covered List only to the extent that it is “capable of—(A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles; (B) causing the network of a provider of advanced communications service to be disrupted remotely; or (C) otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons.”³³

iii. The Commission’s Website Should be Updated

While the Use Qualification is stated on the Covered List on the Commission’s website, the Capability Qualification is not expressly stated -- instead the Covered List merely includes a footnote to the statutory provisions containing the Capability Qualification. A citation to the Act does not provide clear direction to affected parties. The Commission should set forth the criteria for including communications equipment and services as Covered Equipment, so that an affected reader can understand the impact from the four corners of the published Covered List.

In this proceeding, the Commission’s stated goal is a clear understanding for affected parties.³⁴ Hytera suggests that its proposed revisions to the publication of the Covered List on the Commission’s website clarify that the Covered List is expressly limited to equipment and services providing broadband service having a connection speed of at least 200 kbps in either direction, and that meet the Use and Capability Qualifications. This would go a long way toward informing potentially affected parties as to the true effect of Section 1601 of the Act and neutralize marketplace confusion.

³³ Section 1601(b)(2). Section 1608(c) and (d) of the Act specify the criteria for a determination of unacceptable risk to the national security is to be made.

³⁴ NPRM ¶56.

4. Proposed Rule Amendments

a. Section 2.911(d)(5) Certification

Section 2.911(d)(5) of the Commission's rules, 47 C.F.R.³⁵ sets forth the information that must be submitted in each request for equipment authorization submitted to a TCB. In the NPRM, the Commission proposes revising the equipment certification procedures to require applicants to provide a written and signed attestation that, as of the date of the filing of the application, the equipment for which the applicant seeks certification is not on the Covered List.

Hytera urges the Commission to include a mechanism by which an applicant may verify that it has evaluated its proposed equipment and the certifications proposed below may be reliably made as part of the certification process.

Hytera proposes that Section 2.911(d)(5) be amended to include the following attestations as part of the application process:

1. Whether the equipment is being provided by an entity identified on the Covered List.
2. Whether, standing alone, the equipment provides fixed or mobile broadband connection speeds of at least 200 kbps.
3. Whether the equipment is capable of routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles.
4. Whether the equipment is capable of causing the networks of a provider of advanced communications services to be disrupted remotely.
5. Whether the equipment has been deemed to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons by a specific determination made by an appropriate national security agency, as defined by Section 1608 of the Act.
6. Whether the equipment can be used for purposes other than for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes.

³⁵ 47 C.F.R. § 2.911(d)(5).

These attestations track Section 1601 of the Act and ensure that the Commission’s TCB process is consistent. This information is readily available to manufacturers and thus would not add a substantial burden to the equipment certification application. Further, these attestations would be subject to the section 2.911(d)(1) certification to the TCB that all statements in its request for equipment authorization are true and correct to the best of the manufacturer’s knowledge and belief. If necessary, the Section 2.911(d)(1) certification could include, “after due inquiry,” to ensure that each applicant conducts its own due diligence to ensure technical compliance.

b. U.S. Based Responsible Party

As part of this proposed certification process, Hytera fully supports the identification of a U.S.-based responsible party, as contemplated in the revision to **Section 2.1033(b)(1)**. Hytera maintains a significant presence in the U.S. Its U.S. representatives will be responsive to Commission inquiries.

c. The Proposed Revisions to Section 2.906 of the Commission’s Rules- The Supplier’s Declaration of Conformity (“SDoC”) - Exceed the Scope of Section 1601 of the Act

Section 2.906 of the Commission’s rules offers an expedited certification process for certain types of RF devices that have less potential to cause interference. In its proposed revision to Section 2.906 of the Commission’s rules, the Commission proposes to prohibit *any of the entities or their respective subsidiaries or affiliates, that produce or provide “covered” equipment on the Covered List from obtaining equipment authorization through the SDoC process.*

Section 15.101 of the Commission’s rules, 47 C.F.R. §15.101, allows for the streamlined SDoC process for most unintentional radiators. Section 15.201(a) of the Commission’s rules, 47

C.F.R. §15.201(a), allows for the streamlined SDoC process for intentional radiators operated as carrier current systems, devices operated under and consistent with Sections 15.211 (Tunnel Radio Systems), 15.213 (cable locating equipment), and 15.221 (leaky coax system in the 525-1705 kHz band) of the Commission’s rules, 47 C.F.R. §§15.211, 15.213, and 15.221, and devices operating below 490 kHz in which all emissions are below the limits in Section 15.209 of the Commission’s rules 47 C.F.R. §15.209. None of these categories of equipment is likely to ever be Covered Equipment.

Restricting the *entities* listed on the Covered List – and not the Covered Equipment – expands the Commission’s reach beyond the bounds of Section 1601 of the Act without prohibiting the authorization or certification of any threatening equipment. The proposed revision to Section 2.906(c) should be abandoned in whole.

d. Proposed Revisions to Section 2.907: The Complement to Section 2.906

Likewise, proposed **Section 2.907(c)** would expand the requirement of the certification process to all “entities” listed on the Covered List. While the impact of the expansion to *entities* is negligible, the overreach of requiring the certification process for the entities listed on the Covered List, rather than for the Covered Equipment, is again unwarranted and reaches beyond the confines of Section 1601 of the Act.

5. Enforcement Policies

In addition to specific rule modifications, the Commission proposed two new approaches to enforcement of the proposed rules: revocation of existing equipment certifications or authorizations; and a private attorney general type scheme to help ferret out Covered Equipment in use.

a. Revocation of Existing Authorizations.

In Section III(c), of the NPRM, the Commission asks for comment about whether its rules should be modified to enable revocation of existing equipment authorizations. And it tentatively concludes that Sections 2.939(a)(1) and (2) would apply to allow it to revoke authorizations for equipment on the Covered List.

Hytera does not object to the proposed approach but cautions the Commission not to expand its reach beyond the equipment on the Covered List, so as to avoid overstepping the limits imposed by Section 1601 of the Act. Any such revocation process should afford due process to the holders of equipment authorizations. For example, the process should afford the opportunity for holders of threatened equipment authorizations to provide the kind of attestations discussed above to ensure the equipment is within the scope of the Covered List at the outset of the process.

b. Enforcement Reliance on Public Reports

The Commission also asked for comment about whether it should rely on public reports of equipment with parts that might be on the Covered List or of equipment authorizations that should be revoked. Hytera supports the Commission's effort to ferret out issues with insecure equipment on the Covered List. Putting authority in the hands of competitors, however, will allow competitors to abuse the program to their advantage in the marketplace. If the Commission does allow reports from the public, it should require verified documentation that the Use Qualification and Capability Qualification do not apply to equipment that is the subject of a report. Further, based on the amount of misinformation currently in the marketplace surrounding the Covered List, any public reporting rules must allow the imposition of sanctions on those who submit false reports.

Even though it is clear that LMR/DMR equipment is not video surveillance or telecommunications equipment, Hytera has been subjected to vigorous campaigns alleging that its equipment is a security risk. Hytera dealers have submitted comments in this proceeding. Each of them mentioned the backlash he is experiencing because of the imprecise wording used in the Covered List and in the proposed rules.³⁶ Hytera's competitors have used the imprecise language from the Covered List and the Commission's various orders to convince Hytera dealers to bid new customers with their equipment and not Hytera's, even though Hytera equipment might be a better fit for the customer.³⁷ The anticompetitive behavior has gone so far as government procurement offices who, in response to the Covered List and the Commission's orders, now refuse to allow bids from dealers who sell Hytera equipment, even if they sell other equipment and might not propose Hytera equipment in response to the bid request. One state office out west asked that Hytera two-way radios be removed from its contract based solely on federal procurement rules, which do not generally apply to the state entity procurement process, and which relate to Covered Equipment – not two way radios. This underhanded anti-competitive behavior abuses the Commission's processes and will harm the small U.S. owned businesses that form the foundation of Hytera's dealer network.

In light of the disinformation spread in the marketplace, Hytera requests that, in addition to its proposed adjustments to the proposed rules, the Commission state in very clear terms that its Congressional mandate and the rules adopted in this proceeding do not reach PMRS (LMR/DMR) equipment. So long as the equipment is not communications equipment or services capable of routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment transmits or otherwise handles; or causing the network of a

³⁶ Hytera Dealer Letters.

³⁷ *Id.*

provider of advanced communications service to be disrupted remotely, it does not meet the Capability Qualification and is not Covered Equipment. If it is not subject to the restrictions set forth in Section 1601 of the Communications Act, or Sections 1.50002, *et seq.* of the Commission's rules, the mandates evolving from Docket 18-89, or the restrictions adopted as a result of this proceeding.

6. The Commission May Not Exceed the Authority Granted by Congress

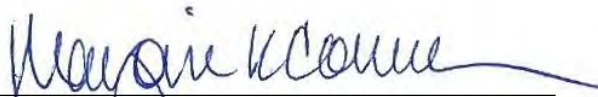
Congress has spoken several times in recent years on its concerns regarding equipment that could harm national security. The Commission's strict adherence to Congressional direction will "ensure that insecure equipment is not left in our nation's interconnected broadband networks" without unnecessarily burdening equipment that is not capable of reaching, let alone, compromising those networks and without leaving the Commission's action open to attack under *Chevron* principles.

Hytera asks that the Commission limit the effect of the proposed rules to Covered Equipment and that it issue a statement that, because of the Capability Qualification, only equipment capable of interconnection with the PSTN or the Internet is qualified to be Covered Equipment.

Respectfully submitted,

HYTERA U.S.

By: _____



Marjorie K. Conner

Its Counsel

mkconner@mkconnerlaw.com

703-626-6980

September 17, 2021

Declaration of Thomas C. Wineland
Vice President of Sales
Hytera US, Inc.

My name is Thomas C. Wineland. I serve as Vice President of Sales for Hytera US, Inc. ("Hytera US"). I write to affirm that I have read Hytera US' comments in *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, ET Docket 21-232. The facts asserted therein are true and correct to the best of my knowledge, information, and belief.

I wanted to take this opportunity to provide more context on how Hytera has been affected by inclusion of Hytera's name in Congress' and the FCC's efforts to protect the US Supply Chain.

By way of background, I have worked in the land mobile radio industry for over thirty years. I joined Hytera about five years ago. I was drawn to their commitment for quality and value for our customers and to their local dealer network. I was also aware of their commitment to serving the communities their local dealers serve. Hytera US' philanthropy is remarkable; it drew me to Hytera.

I have served on the IWCE advisory board and on EWA's Board of Directors, among other industry leadership roles.

I have been working with our US dealer network during the difficulties caused by Hytera's listing on the Covered List, first published in November 2018, in the 2019 NDAA. Hytera was confused by the listing because we were listed as providers of video surveillance and telecommunications equipment. We don't make or sell either of those things. Hytera was blindsided by its inclusion on the Covered List.

Hytera is a small company in comparison to the other companies on the Covered List. Our local dealers are independent. Most of them represent other manufacturers, with Hytera's blessing. Most of our local dealers are small, family-owned operations. Many of our dealers are veterans; many are women. I have a close relationship with all of our dealers and work with them to increase their sales.

As you can imagine, the Covered List has destroyed our dealers' ability to sell Hytera. Even if they can convince their customers that the two-way radios they plan to buy are not on the Covered List, the customers, in turn, answer to their bosses. They tell the dealer they "just can't take the risk" that the FCC will demand that Hytera equipment be removed and replaced.

Our dealers and their customers do not have access to communications lawyers who read the Communications Act and the FCC's rules and interpret the nuances. They see Hytera's name on the Covered List and choose a different manufacturer. One state agency even has Hytera representation as a disqualifying factor for its bidders on a request for proposals. The program asks if the bidder represents Hytera – not if the bidder plans to bid Hytera products, just if the bidder represents Hytera. Certainly this anti-competitive impact in the two-way radio marketplace was not what was contemplated in creating the Covered List.

Hytera US is a good citizen in each of its communities. It does not market broadband equipment in the US. A clarification that the Covered List reaches only broadband equipment would give Hytera the ability to neutralize the Covered List's anti-competitive impact and allow the free market to operate.



Thomas C. Wineland
Vice President of Sales
Hytera US, Inc.

September 17, 2021

Attachment 1



Hytera America Donates Radios to Hatzalah Emergency Services to Fight the COVID-19 Pandemic in New York

SOCIAL RESPONSIBILITY



Irvine, CA, April 6, 2020 - Hytera America, in partnership with Abest Communications, has donated X1pi DMR radios to Chevra Hatzalah to help their volunteers communicate and save lives in New York City, the national epicenter of the COVID-19 pandemic.

Hatzalah is the largest volunteer emergency medical service (EMS) in the world with operations in 16 countries serving mostly Jewish communities. Hatzalah was originally founded in Brooklyn, New York, where they are known as Chevra Hatzalah, and are currently serving the entire New York City region. VHF two-way radios provide lifesaving communications to Hatzalah's 1,300 volunteer EMTs, dispatchers, and paramedics. They respond to over 70,000 calls each year with private vehicles and a fleet of more than 90 ambulances.

"We are at the forefront of the fight against COVID-19. Our volunteers are inundated with emergency calls during this period. Generosity such as yours encourages our volunteers to keep operating at this challenging time – often at risk to their own personal safety", said Abraham Wurzberger, Executive Director of Chevra Hatzalah. "Your generous donation will directly contribute towards Hatzalah's life-saving mission."

Attachment 2



Hytera America Donates Radios to Northwestern Medicine Lake Forest Hospital

S O C I A L R E S P O N S I B I L I T Y



Irvine, CA, September 2, 2020 - Hytera America, in partnership with Alpha Prime Communications, has donated fifteen PD602i DMR radios to Northwestern Medicine Lake Forest Hospital to help them coordinate resources with efficient communications to respond to the COVID-19 pandemic.

The Northwestern Medicine health system serves patients across Chicago at ten hospitals, including Lake Forest Hospital, a 198-bed acute-care facility with an emergency room, eight operating rooms, and five pavilions for inpatient and ambulatory care. In March of 2018, Lake Forest Hospital completed nearly 500,000 square feet of new construction on its 160-acre campus, replacing the existing hospital building that was over 100 years old.

Alpha Prime Communications, a leading wireless communications dealer, has been providing radio communications equipment and services to Lake Forest Hospital for more than 13 years. Alpha Prime conducted an extensive review of the new hospital's communications needs and recommended the Hytera Digital Mobile Radio (DMR) trunking solution with DMR portable radios and mobile radios for dispatch services.

Alpha Prime mitigated any coverage issues that might arise with the sprawling campus by designing and installing a Distributed Antenna System (DAS) to ensure campus-wide coverage for the new Hytera 2-site, 6 channel DMR trunking system. Users on the system include the maintenance, engineering, security, administration, emergency, grounds, and environmental services teams.

"Chicago is experiencing one of the worst COVID-19 outbreaks in the country," said Don Colbert, the Director of Facilities at Lake Forest Hospital, "The generous donation from Hytera and Alpha Prime has helped our different departments coordinate our pandemic response to provide treatment to the growing number of COVID-19 patients."

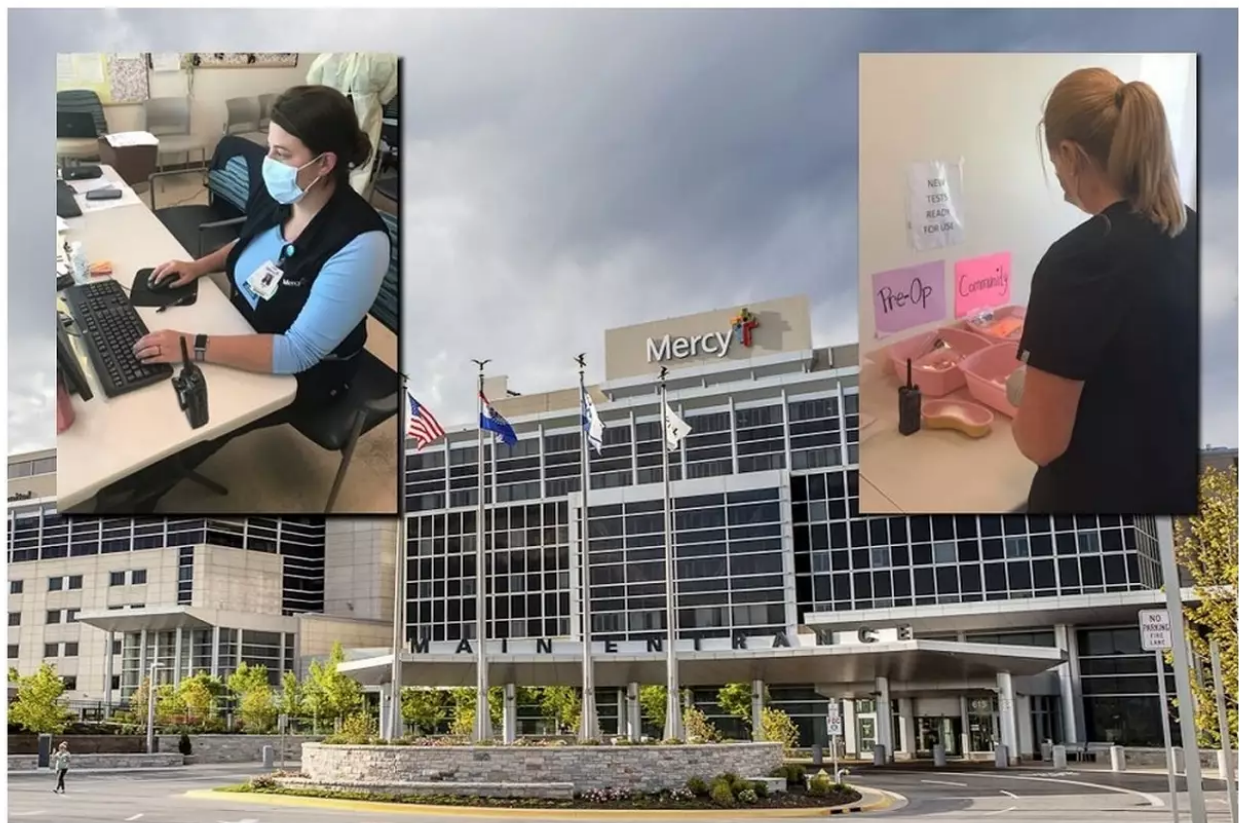
"The donated radios are used to supplement over one hundred Hytera portable radios being used on the Lake Forest Hospital campus every day," said Andy Kerman, the Sales and Service Manager at Alpha Prime. "Along with Hytera, we are dedicated to providing two-way radio solutions to the

Attachment 3



Hytera America Donates Radios to Mercy to Fight the COVID-19 Pandemic in St. Louis

S O C I A L R E S P O N S I B I L I T Y



Irvine, CA, August 14, 2020 - Hytera America, in partnership with Warner Communications, has donated PD782i DMR radios to Mercy Hospital St. Louis to help provide testing and save lives during the COVID-19 pandemic.

The Mercy health system was founded by the Sisters of Mercy in 1986. Today, Mercy includes more than 40 acute care, managed and specialty hospitals, 900 physician practices, and outpatient facilities, and 2,400 Mercy Clinic physicians in Arkansas, Kansas, Missouri, and Oklahoma. Mercy also has clinics, outpatient services, and outreach ministries in Arkansas, Louisiana, Mississippi, and Texas.

Mercy Hospital St. Louis was the first organization in the state to offer drive-through testing. Mercy was also the first hospital in the state to have a patient test positive for COVID-19, followed by an influx of symptomatic patients. The challenge was to prevent strain in the Emergency room and to isolate infected patients. Andrew Blevin, Mercy's Regional Director for Emergency Preparedness, helped expand the testing facilities and establish respiratory care clinics to provide intermediate patient care, prevent exposure risk, and reduce the pressure on the area's emergency rooms. He also worked to develop the Mercy-wide policies and procedures, "Whole of Mercy Response to COVID-19."

Attachment 4



Hytera Provides Push-to-Talk over Cellular Communications to Wreaths Across America

SOCIAL RESPONSIBILITY

IRVINE, CA – December 15, 2020 – On Tuesday, December 15th, Wreaths Across America started the annual caravan to deliver wreaths to Arlington National Cemetery on National Wreaths Across America Day on Saturday, December 19th. The caravan started in Maine and will travel across six East Coast states, lead by Grand Marshal Cindy Tatum, the National President of American Gold Star Mothers Inc. (AGSM). Escort participants include American Gold Star Families, Blue Star Families, veterans, volunteers, and supporters from across the country.

The logistic support for the annual caravan is coordinated by Chief Janine Roberts of the Westbrook Police Department. The caravan is escorted by Commander Trooper Robert Burke of the Maine State Police Honor Guard, who will manage convoy operations along the route, along with eight officers from five different police departments.

Hytera provided 35 PNC370 Push-to-Talk over Cellular (PoC) radios to Wreaths Across America that enable communications between caravan drivers, police escort vehicles, volunteers, and staff. The radios are connected to the Hytera HALO cloud-based server and the T-Mobile LTE network using SIM cards donated by Choice IoT through their VP of Sales Jim Vicatos. Both the nationwide T-Mobile and Hytera HALO PoC services were donated to Wreaths Across America.

"The radio system donated by Hytera and Choice IoT is integral to our convoy participants relaying pertinent information during the caravan," said Chief Roberts. "They also enable our safety briefings that ensure safe COVID-19 practices and social distancing."

Due to COVID-19 safety guidelines, limits were placed on the size of the caravan and the number of stops along the route. Most of the trailers of wreaths have arrived separately at Arlington National Cemetery, and the U.S. Army Military District of Washington and the 3d U.S. Infantry Regiment will safely lay and recover approximately 267,000 wreaths to honor our nation's heroes and their family members. The cemetery will be closed to the general public from December 13th to the 18th, but family pass holders are welcome to visit and place their private wreaths and flowers. On Saturday, December 19 a small group of Wreaths Across America team members will place wreaths in a designated section of the cemetery.

About Wreaths Across America

Wreaths Across America is a 501(c)(3) nonprofit organization founded to continue and expand the annual wreath-laying ceremony at Arlington National Cemetery, begun by Maine businessman Morrill Worcester in 1992. The organization's mission – Remember, Honor, Teach – is carried out in part each year by coordinating wreath-laying ceremonies in December at Arlington, as well as at more than 1,900 veterans' cemeteries and other locations in all 50 states and overseas.

For more information, please visit www.wreathsassamerica.org

About Hytera America

Attachment 5

Innovation keeps Hytera at global forefront: founder

Writer: Chen Qingzhou Zhang Qian | Editor: 杨梅 | From: | Updated: 2018-10-31

SINCE he first attended an international exhibition in the United States in 2001, Chen Qingzhou, founder and chairman of the board of Hytera Communications Corp. Ltd., has been upholding the maxim “Think Globally, Act Locally,” which has helped his company take a leading position in the global market for private communication networks.

Hytera is a listed company headquartered in Shenzhen. Established in 1993, the communication network solution provider is dedicated to providing customized and complete professional communications solutions to help governments and public security, utility and transportation enterprises improve organizational efficiency.

In 1992, when Shenzhen became a dreamland for many young entrepreneurs thanks to Deng Xiaoping’s famous speech during his tour of South China, Chen also came to Shenzhen to find his living.

A rental store in Huaqiangbei was where Chen started trading imported walkie-talkies. After diving deeper into the industry, Chen, from Fujian Province, decided to manufacture the best walkie-talkie in China.

Chen founded his start-up with a team of only five people a year later and has been focused on the research and development of private communication networks ever since.

“I have been determined to achieve big goals since I was young and luckily I had the fortune of living in the right time for development,” Chen recalled in a recent interview. Shenzhen had developed a technology park at that time, which provided a supportive environment for Chen and his company with various types of professional training and salons.

Two years later, Chen and his team had invented China’s first self-developed professional wireless private communication equipment, the C160 walkie-talkie. Three years after that, Chen had achieved his dream of “producing China’s best walkie-talkie.”

The company’s global journey started in 1997, when Chen paid his first visit to the United States, where he planned to begin expanding his company into global markets.

“I remember the price for a can of cola was US\$2.5, which equaled to more than 20 yuan at that time, so I was sure that entering the U.S. market would bring high profits for my company,” said Chen.

However, getting recognized in the U.S. market was not easy. Chen realized that only high-quality products and services could earn his company a place. Therefore, Chen and his team

focused on improving the quality of their products and continuing R&D to meet the U.S. standards for private communication network solutions.

Always focused on innovation, Hytera insists that continuously investing a lot of funds in R&D has probably been the main impetus for driving innovation among enterprises over the past decade. The company's investment in R&D accounted for 17 percent of its total revenue in 2017, and 41 percent of the company's staff are R&D personnel.

Hytera has established 10 R&D centers inside and outside of China, specifically in Shenzhen, Harbin, Nanjing, Hebi and Songshan Lake area in Dongguan, as well as Bart Meade in Germany, Cambridge in the United Kingdom, Zaragoza in Spain, and Vancouver and Toronto in Canada.

Focused on customer value, Hytera has constructed marketing and service networks globally and has more than 90 branches and professional personnel from more than 40 countries and regions around the world.

It has established long-term and stable cooperative relationships with many global dealers and partners, providing products and solutions for government and corporate customers in more than 120 countries.

In recent years, Hytera has been active in providing support and event security for major international activities, such as the G20 summit, the BRICS summit and the Rio Olympic Games, earning the trust of an increasing number of government and corporate customers.

Attachment 6

ECFS Express

1
COMMENT

2
REVIEW

3
CONFIRMATION

Proceeding: 21-232

Confirmation #: 2021082448381105

Submitted: Aug 24, 2021 5:02:09 PM

Status: RECEIVED

Name(s) of Filer(s) MicroMagic Radio Communications

Primary Contact Email felix@micromagic2way.com

Address 2640 East 14th Street Unit C2, Brooklyn, NY, 11235

Brief Comments: By the way of introduction, MicroMagic is an authorized two-way radio dealer and system integrator since 1993 with over 120 years of combined experience in the industry. We are a small business providing services to the New York tri-state area and work with NYC, NYS and Federal agencies (VA, GSA), major hospitals, educational institutions (including city (CUNY) and state (SUNY) universities and colleges), hotel chains, construction companies as well as commercial and residential properties. MicroMagic has been a Hytera dealer since 2010. A large portion of our customers use Hytera products, and we have always received positive feedback about them. In my years as a dealer, I have only seen Hytera to provide good products and effective support for their equipment. None of the Hytera systems we implement are ever connected to PSTN or broadband. Even in the case that a customer request such a connection, this requires additional non-Hytera (3rd party) equipment to be added to the system. I would like to bring to your attention that since Hytera has been placed on the NDAA/SNA Covered Lists our competitors have begun using this information to scare customers away from Hytera products. Recently, we have seen some previously approved orders for Hytera products be canceled and the explanation given was that the FCC no longer allows Hytera products to be sold in the US. I would respectfully request the FCC to reconsider their decision about placing Hytera on this list. Sincerely, Felix Vayner, Owner, MicroMagic Co. Inc.

Email Confirmation Yes

East Mountain Communications

2617 Wingdale Mountain Road
Poughquag, NY 12570
845-485-3335
Fax-845-485-8920

August 25, 2021

Marlene H. Dortch, Secretary
Federal Communications Commission
45 L Street NW
Washington DC, 20554

RE: ET Docket 21-232 and EA Docket 21-233

Dear Ms. Dortch,

East Mountain Communications has been in business for 25 years specializing in two-way radio communications and has been a Hytera Dealer since 2016. We currently have an 8 site, DMR Tier III Trunk Light System which services 5 of the largest school districts in Dutchess & Ulster Counties in NY, in addition to local commercial businesses.

Although we are a small company with 4 employees (all of which are US citizens, most with families) we are an industry leader in our area. This is in large part due to the outstanding commitment to us by Hytera. They have been a driving force behind the continued success of our company. I firmly believe that without the product, commitment to service and support by Hytera that East Mountain Communications would have closed their doors. We pride ourselves on the service that we provide to our customers, but this can only be accomplished with quality products. I have the utmost faith in the products from Hytera that I sell my customers and Hytera has proven time and time again that they are committed to quality equipment. The equipment that my company and my customers have come to rely on are not interconnected. The only way to accomplish an interconnected system when requested by a customer is through third party equipment.

We have found that with the 3-year warranty, outstanding performance, and quality that Hytera products possess they have become popular purchases. Unfortunately, our company has experienced the effects of a whisper campaign launched against Hytera. Many of our customers have received mail transmitting copies of news articles identifying Hytera as a company on the NDAA/SNA Covered lists. My customers and potential customers have expressed concerns about investing into equipment that

is supposedly on the Covered Lists. They often ask for alternate quotes without Hytera equipment. This is difficult to achieve as Hytera's products are some of the best in the business which we rely on greatly.

Since the Public Notice (DA 21-309) that included the NDAA/FCC Covered List was put out we have been told that people and companies are not to consider Hytera because they are a security risk. Competitors appear to be using this FCC Public Notice to sway customers and potential customers from our DMR Hytera system. The Notice references that the risk is with "video surveillance and telecommunication equipment". I have never known Hytera to sell or advertise video surveillance equipment and the only telecommunications equipment I am aware of Hytera selling is the LMR which is a closed system controlled by the owner, not Hytera.

As a very proud American, Small Business owner and retired Law Enforcement Officer I have never seen anything to warrant Hytera US to be added to any sort of security risk list for the equipment it sells.

Thank you,

Ralph Mondello

Ralph Mondello
President



Aug. 26, 2021

Federal Communications Commission
Attn: Marlene H. Dortch, Secretary
45 L Street NW
Washington, DC 20554

Dear Ms. Dortch,

Re: ET Docket 21-232 and EA Docket 21-233

We are writing this to you in concern that Hytera two-way DMR radio equipment may be put on a list of equipment that is considered a security risk if sold in the United States.

We are a small two-way business in rural Missouri, operating since 1980. I have a Professional Engineering license and am quite knowledgeable about the products in our industry. When I examined the Hytera line of radios back in 2008, I and key employees thoroughly looked them over to determine if they were of the quality we required. I immediately signed up to be a dealer, due to the quality of the equipment, the pricing structure and the warranty support they offered. Their support, both from the sales standpoint and service is second to none.

We have represented other lines of equipment and Hytera support ranks right up there with the best. We have found the Chinese people to be very cordial and helpful.

I also happen to be a disabled Vietnam era veteran, who loves this country and would never represent a foreign product that was a security risk to this nation.

We and other Hytera dealers around the country are experiencing backlash from potential as well as existing DMR customers over the rumors that Hytera land mobile equipment is and should be on this security threat list. I believe, it is a classic case of competitive outcry in our industry.

Thank you for your attention to this matter.

Sincerely,

Michael D. Salmon,

President
Communications Associates

HARRIS
NETWORK SOLUTION
PROVIDER

www.CommAssocRadio.com

3343 South Scenic Ave.
Springfield, MO 65807
Phone (417) 882-1401
Fax (417) 883-4948

Hytera



September 7, 2021

Marlene H. Dortch, Secretary
Federal Communications Commission
45 L Street NW
Washington, DC 20554

Re: ET Docket 21-232 and EA Docket 21-233

Dear Ms. Dortch:

I'm writing to protest Hytera Communications Corporation's inclusion on the FCC's Covered List as an extension of the Secure Networks Act (DA 21-309). The notion that Hytera's products and services "pose an unacceptable risk to the national security of the United States" is absurd.

My firm, Diversified Communications Group (DCG), has been in the radio communications business for more than 30 years and we have been a Hytera client for more than a decade. We have installed and distributed Hytera products to dozens of Fortune 500 companies and small to medium-sized businesses. Hytera products are not "video surveillance or telecommunication equipment" – they are two-way radio communication devices that operate in closed systems. The hardware involved is not connected to the internet and does not transmit any sensitive or proprietary data.

Hytera's high-performing product portfolio and competitive pricing has helped our business thrive. We operate in an industry dominated by one large manufacturer. Hytera is a needed counter balance to this domination and is one of the few suppliers that actually delivers true business partnership to independent firms like mine.

It seems that Hytera has been lumped in with other Chinese companies on the Covered List simply because they happen to manufacture electronics in the same country. This is a wrong that should be righted. Hytera is not a national security risk. They are an essential business partner to radio companies throughout the U.S.

I respectfully request that the FCC reconsider Hytera's inclusion on the Covered List and remove them from it.

Sincerely,

A handwritten signature in blue ink, appearing to read "Ryan J. Holte", is written over a light blue horizontal line.

Ryan J. Holte, CEO



September 14, 2021

Marlene Dortch

FCC

45 L Street, NW

Washington, DC 20554

Re: ET Docket 21-232 & EA Docket 21-233

Ms. Dortch,

As a provider for our Pennsylvania state contract, we were disappointed to learn that Hytera was singled out as the only radio manufacturer not allowed on the list of two-way communication options.

We've been a servicing dealer for radio products for nearly 39 years. Our dealership has come to be known as the go-to for schools and extended living facilities who are looking for reliable communications to utilize for their safety and security programs, which have become paramount in the 21st Century. A number of manufacturers have price points above what many budgets can bear, but Hytera stands at the crossroads of the reliable technology they need and the cost they can afford. I can tell you with certainty that the students and staff at the facilities we serve, are safer today because of the Hytera products and infrastructure they were able to put into place.

It is our sincere wish that, in the interest of safety, we will see Hytera among the counted on our State contract list of manufacturers in the near future.

Sincerely,

A handwritten signature in cursive script, appearing to read "Chuck Freese".

Chuck Freese
President,
FreCom Inc.

GCSEAC, Inc.

PO Box 5151
Martinsville, VA 24115

276.632.9700

www.gcseac.com



September 11, 2021

Marlene Dortch
FCC
45 L Street, NW
Washington, DC 20554

Re: ET Docket 21-232 & EA Docket 21-233

Ms. Dortch,

This letter is to express my concern for Hytera being on the covered list of the Secure Networks Act (DA-21-309). Our company has implemented many Hytera two-way radio systems for a variety of customers from hospitality (restaurants) to schools to distribution centers. These are dedicated systems and are not connected to an internet or telephone connection. They are vital parts of the customers we serve.

I think there has been much fanfare projected by one manufacturer that does its best to intimidate and dominate the market in any manner they can. They project an image of perfection and compliance in an effort to stifle anyone not part of their dealer network, such as companies like ours.

We have been in business nearly 30 years and this inclusion has caused us some issues in selling Hytera when it does not even apply to us in our application and does not apply with Hytera two-way radio systems.

Please reconsider removing them from the "list" as a security risk.

Thank you,

A handwritten signature in blue ink, appearing to read "Giles Smith", with a long horizontal flourish extending to the right.

Giles Smith
President



8534 Terminal Road
Suite B
Lorton, VA 22079
703-337-4637

September 13, 2021

To whom it may concern,

Metrotalk Inc. is a HYTERA dealer serving the Washington DC, Virginia, and Maryland markets. Since becoming a dealer in June 2009, the working relationship has been excellent. HYTERA has provided Metrotalk Inc. with the training and technical support we needed to properly represent their products. They never requested we stop selling a competitor's products to have access to HYTERA equipment.

Our goal has always been to provide our customers with the best product available in the market while meeting their budgets. Due to this philosophy, we represented different two-way radio vendors. Each vendor offered a unique product or feature our customers wanted or needed. As we introduced the HYTERA equipment to our customers, they were able to use the HYTERA radios and repeaters with the existing two-way radios we had previously sold them. The equipment worked seamlessly and as the customers used the HYTERA radios they noticed one thing, the HYTERA equipment offered better features, functionality, ruggedness and most importantly, it was very reliable. The HYTERA equipment was so reliable that our customers would ask us to just sell them HYTERA and not the other brand we had been providing. As time went by, our customers' referrals became an important source of new customers. We also faced cancellation from one of our long-term suppliers after they were purchased by Motorola. First our direct relationship with the manufacturer was relegated to a reseller. Then, for no reason the reseller terminated our resale agreement. At the time they were still our primary product line.

The use of HYTERA two-way radios and repeaters in our rental department allowed us to introduce the product to the event industry. The event industry relies on two-way radios for event planning and execution. The HYTERA two-way radio equipment was first received with the typical skepticism every new product receives. The event customers were concerned about reliability and ease of use. It did not take long for HYTERA to not only be the preferred two-way radio for our event clients, but they also started purchasing the HYTERA radios and repeaters for their in-house event staff and the venues they offered for events. This allowed Metrotalk Inc. to be able to hire delivery personnel and support staff. We grew from just 2 employees to 4 with the help of HYTERA and their excellent product line.

As the years passed and we introduced HYTERA to more private customers, rental customers, event industry, school districts and Federal agencies, all were happy to have a product that solved their two-way communication problems, reliability concerns and budget constraints at the same time. Most were bought as standalone operations. The two-way radios and repeaters were purchased for the exclusive job of providing communications within a federal building, local public school, stadium, concert hall, convention center or office building. All the equipment was FCC licensed and when requested, the specification test reports were provided to the customer by HYTERA.



8534 Terminal Road
Suite B
Lorton, VA 22079
703-337-4637

As the DMR standards were approved for the use of new technologies, HYTERA introduced those features and functions into their products as well. Some required the customer to purchase a special license and their equipment to be upgraded for the feature to work. One feature which offered great functionality at a reasonable cost was the ability to connect multiple buildings into one network, using the IP (Internet Protocol) standard and readily available internet connectivity commonly used in buildings. HYTERA offered our customers the ability to link multiple locations allowing them to be able to call a staff member in one building from another building across town or state. School districts were considering it to connect their schools into a network which would allow school principals to talk to other principals or maintenance personnel during emergencies.

The HYTERA repeaters offered the IP technology to link the buildings but not the ability to do so without external equipment which HYTERA did not provide and does not provide to this day. The IP linking of separate locations relies on the customer provided routers, servers cabling and internet provider. HYTERA does not offer any of those critical infrastructure devices and or services.

That is why, it came as a shock when HYTERA was included in the NDAA/SNA covered list. Immediately, Metrotalk Inc. was called into meetings with our Federal, State and University customers as well as our private sector customers that had been using HYTERA to perform their services to their FEDERAL and State clients. They wanted to know why HYTERA was listed and how it would affect their business and budget. All we could tell them was that it did not make sense for HYTERA to be included with Huawei, a cellular infrastructure provider. They knew it made no sense since the majority were using their two-way radio equipment as a stand-alone system and not connected to the IP (internet system) in any way. Most of our customers' repeaters do not have the IP license active which makes it impossible for the repeater to work even if it is connected to an IP line.

The next part of the conversation was how to postpone the inevitable replacement of all HYTERA two-way radios with other more expensive equipment. Some Federal agencies requested an extension. Some schools decided it was too much of a hassle and started to budget to replace the HYTERA equipment with available suppliers. Some had purchased HYTERA after multiple bids had been requested and having determined that HYTERA offered the best price and functionality. These same customers are now faced with having to pay much more for similar equipment they had declined to purchase in the past due to the high cost.

Our rental department recently, after 16 months of little to no rental business due to Covid-19, received a rental request. There was one catch. The customer had demanded from our reseller that HYTERA two-way radios were not to be provided. This came as a shock to us as more than 70% of our rental equipment is HYTERA. We looked at the requirement to not use HYTERA as not being rational. Firstly, since our reseller had been renting HYTERA from us for all their key events for the last 5 years. Secondly, what logical reason did the customer have for not wanting the HYTERA radios we offered. There was no



8534 Terminal Road
Suite B
Lorton, VA 22079
703-337-4637

technical reason for the request. Since we must provide what the customer requested, we quoted old radios that were not going to offer the same coverage as the HYTERA radios.

We have also stopped offering HYTERA whenever we come across bid requests from FEDERAL, STATE or Local government and School districts. We know that once HYTERA is offered, it will be disqualified. We only offer HYTERA if it is requested by name.

I hope my letter offers you a glimpse into the damage the NDAA/SNA list has done to our customers, to us, and to HYTERA. Keeping HYTERA on the list is increasing the cost to everyone that relies on two-way radios. It also allows the main two-way radio provider in the USA to increase their market influence.

Francisco Sampedro

Francisco Sampedro
President

ALPHA PRIME COMMUNICATIONS

5646 W Monee Manhattan Rd · 708-534-8030

Marlene H. Dortch, Secretary
Federal Communications Commission
45 L Street NW
Washington, DC 20554

Re: ET Docket 21-232 and EA Docket 21-2

Dear Ms Dortch,

I am a Hytera dealer in the Midwest. We work with many radio manufactures and have for many years. We started working with Hytera when Motorola started raising its prices on the radios our customers needed to do their jobs. We have found them to be reliable and sturdy. They provide a value for the price charged. Most of our customers are Schools, small Manufactures and small business in general.

We do not sell networked equipment and have no Hytera video products and can not understand why they would be included in a ban for this type of product. This far reaching ban threatens many of our customers day to day communications and safety. One of our larger logistics companies will need to spend about \$100,000.00 to replace their radios that have worked well and required little or no service.

Please do not paint us and Hytera with a sweeping ban when you consider your decision in this matter.

Respectfully,
John Hickey
General Manager
Alpha Prime Communications
5646 W. Monee Manhattan rd
Monee, IL 60449



1219 Price Plaza, Suite 200
Houston, TX 77449
Phone: 281-616-7244
jmills@voceon.com

August 9, 2021

Ms. Marlene H. Dortch,
Secretary
Federal Communications Commission
45 L Street NW
Washington, DC 20554

Re: ET Docket 21-232, and EA Docket 21-233

Dear Ms. Dortch,

My name is Joel Mills and I am the General Manager for Voceon Digital Radio Communications in Houston Texas. I have been working here since 2016 and have been in the communications industry for 29 years. Our company employees 9 people and we also have 6 sub-dealers under us that have numerous employees of their own. Our company, as well as our sub-dealers are run and operated by U.S. Citizens who provide Hytera products and services for the Texas and Louisiana markets. Hytera makes up to 100% of the sales for 2 of our sub-dealers and is 90% of our sales. Hytera has given us the opportunity to save customers money, downtime, and costly repairs. We have Hytera radios deployed at many large corporations, small businesses and major school districts including one of the largest in the Greater Houston Area. Their radios are not only offered at an excellent price point but have numerous features that allow companies and schools to provide the security they need in this day in age

It has been said that the Hytera product is a security risk and that government and private sectors should not purchase Hytera products since the NDAA/FCC put it on public notice DA 12-309. Our competitors have taken full advantage of this and have done everything in their power to discredit Hytera, their dealers and their sub-dealers with false and misleading information. This has been a time consuming, ongoing battle and a struggle however, we still succeed in providing our customers with the exceptional product produced by Hytera. The fact is, the Hytera product is a LMR closed system and is controlled by the user. In some rare cases, audio needs to be carried via network which requires third party equipment which is not available through Hytera. All of the Hytera equipment that we and our sub-dealers sell is 95% in house and does not connect to any network whatsoever. I have found no evidence that support any of the allegations made claiming that Hytera products have the capability of spying or taking control of any of the end users products. I feel Hytera products should not have been placed on NDAA/FCC public notice DA 12-309.

Hytera has gone above and beyond in helping our fellow Americans in their time of need. They have provided free radios to numerous organizations in areas affected by such tragedies as hurricane ravaged communities, communities that experienced deadly flooding and has provided free radios to hospitals that are overwhelmed by the pandemic. Voceon, just sent free Hytera LMR radios to Louisiana due to the two hurricanes that have devastated Americans once again. In closing, Hytera provides superior support for their dealers going above and beyond to ensure the satisfaction of our customers. I would like to thank you for reading this letter that I have provided you, and you are always welcome to contact me.

Thank you,

Joel Mills



BAKER'S COMMUNICATIONS, INC

POST OFFICE BOX 3179
LAKE CITY, FLORIDA 32056-3179

386-752-6494 TEL
800-437-2346 WATTS

August 9, 2021

To whom it may concern;

Baker's Communications Inc. is a 47 year old two way radio communication company, employing 15 people (all of which are US citizens with families). We have been a Hytera US Dealer since 2008 just after they started operations in Miami Florida.

We found that the Hytera LMR radios, not only has outstanding performance but outstanding quality. We found that the radios with their 3 year warranty, sells well in our market which comprises of Public Safety and large industrial companies.

Since the NDAA/FCC Covered List was put out thru the Public Notice (DA 21-309), we have been told that they (people from agencies and/or companies) are not to consider them for radio systems because they had been told that Hytera was a security risk.

However, the Notice advises that risk is with "video surveillance and telecommunication equipment" which I have never heard, read or seen any Hytera web sites showing, advertising the sale of or offering of video surveillance equipment. As far as telecommunication equipment, the only items Hytera sells is LMR which by its nature is a closed system which the owner or user controls.

We have quoted some interconnected items but these rely on third party items such as Cisco routers and switches.

We have just experienced another example of last minute cancelation from a bid (an Electric plant), after they were told that Hytera was a risk, even though one of their other facilities uses a Hytera system.

Competitors seem to be using the FCC Public Notice as a whisper campaign against our DMR offered product Hytera.

I can only attest to what I have experienced. In my 47 years in the two way profession, land mobile is and will remain a closed systems with any connection to the outside world having to be done by a third party, as I stated above.

As a very loyal and proud American, I have not seen anything to warrant Hytera US land mobile to be on the security risk list of equipment.

Thank you,

Douglas Baker

Douglas Baker
President



August 9, 2021

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554

Re:

Dear Ms. Dortch:

We are a dealer of two-way radio products based out of St Louis, Missouri. Our company has been in business since 1962. We are directly involved in the sales, installation, and service of the products we represent. Our company and subsidiaries employ 40 people. Every one of those 40 people are US citizens. We are a dealer for multiple lines of products including Hytera.

I am concerned that the federal government and the FCC are unreasonably targeting Hytera products as a security risk to users. This leaves potential purchasers with the impression that these products are used by the Chinese government to spy on users. This could not be farther from the truth. The Hytera two-way radio equipment is usually installed as a closed system. The system works very well without any connection to the public telephone network or the internet. In the rear case where we (and our customer) choose to carry the audio over the internet, we are required to use third party, non-Hytera equipment to accomplish this task.

We have sold, serviced, and installed Hytera two-way radio products we see no evidence that their equipment is able to be used as a spy tool for a foreign government. The analog and DMR equipment are designed as a closed system with any need to connect to the public telephone network or the internet to operate. 90% of our Hytera DMR sales fall into this category. In the case where we decide to use internet connectivity to transport audio traffic between repeaters, we use third party devises, not supplied by Hytera, to switch and route the traffic.

In our markets, there are competitors using the documentation of the FCC proposed rulemaking to scare end users. We have direct experience with numerous customers who have stopped purchasing Hytera products because of these unsubstantiated government accusations and proposed rulemaking.

Our experience with Hytera has shown them to be a big supporter of us as a US owned and operated small business. Most radio suppliers in our industry have an arm where they will sell

Attachment 7

Technology

FCC Proposes Ban on Chinese Surveillance Cameras, Other Products

By [Todd Shields](#)

June 16, 2021, 9:43 PM EDT

Updated on June 17, 2021, 11:07 AM EDT

-
- ▶ FCC moving to restrict U.S. market access for Huawei, others
 - ▶ Oppression of Uyghurs, security flaws cited by U.S. officials
-



U.S. FCC Proposes Ban on Chinese Surveillance Cameras

U.S. regulators proposed a ban on products from [Huawei Technologies Co.](#) and four other Chinese electronics companies, including surveillance cameras widely used by schools but linked to oppression in western China, stepping up pressure on tech suppliers alleged to be security risks.

[Hangzhou Hikvision Digital Technology Co.](#) and [Dahua Technology Co.](#), whose cameras can be found in U.S. schools and local government facilities, were targeted in an order the [Federal Communications Commission](#) adopted in a 4-0 vote on Thursday. Also named in the order were telecom giant [ZTE Corp.](#) and two-way radio maker [Hytera Communications Corp.](#)

The order would forbid U.S. sales of specified telecommunications and surveillance

equipment from the companies. The action begins a period of review before a final vote on the matter.

“We are taking direct action to exclude untrusted equipment and vendors from communications networks,” said FCC Acting Chairwoman Jessica Rosenworcel.

In the proposal, the FCC said it also may revoke its previous authorization for equipment from the companies, a step that could force schools and other U.S. customers to replace the camera systems.

READ MORE

[How Huawei Landed at the Center of Global Tech Tussle: QuickTake](#)

[Why 5G Phones Are New Focus of Freakouts About Huawei: QuickTake](#)

[Huawei's Ambitious Post-Trump Reinvention: Fully Charged](#)

The FCC action represents another step after “years of Huawei warnings,” said Derek Scissors, a resident scholar at the American Enterprise Institute whose focus includes U.S. economic relations with Asia. “Any recent purchasers of Chinese telecom equipment who have been expecting years of use and now must exchange equipment should have known better.”

In its draft order, the FCC didn’t say how quickly affected gear would need to be removed, and it asked for comments on the “appropriate and reasonable transition period.”

“This could include a transition period for non-conforming equipment,” according to the order.

The FCC, Congress and the [White House](#) have pushed to ensure Huawei and ZTE gear isn’t used in U.S. networks, citing risks of cyber-espionage that the companies deny. In 2018 Congress voted to stop federal agencies from buying gear from the five companies now subject to FCC pressure. Last year the agency put the companies on [a list](#) of providers whose products are deemed a national security threat.

“The FCC must do all it can within its legal authority to address national security threats,” Rosenworcel, a Democrat, said in a statement before the vote. The move begins a period of review and possible revision before a final vote. There is no date set for that.

Congressional Action

Huawei, which markets phones in the U.S., said in a statement that the proposed FCC steps were “misguided and unnecessarily punitive.”

Hikvision in an email said its designation as a threat isn’t substantiated, and it “strongly opposes” the FCC measure. Dahua said it “does not and never has represented any type of threat to U.S. national security.” It called the FCC’s proceeding “unwarranted.”

Hytera said its products “don’t impose any threats to any country’s national security” and called the FCC’s approach inconsistent with the U.S. government’s standard practice for evaluating and mitigating risk.

President Joe Biden has continued to pressure China following tense relations with that country under his predecessor, Donald Trump. In recent weeks Biden has urged allies to confront China on alleged human rights abuses, including at the recently concluded Group of Seven summit in the U.K.

Congress may weigh in, too. The FCC would be prohibited from reviewing or issuing new equipment licenses to companies on the agency’s list of suspect equipment or services under a bill announced June 15 by Representative Anna Eshoo, a California Democrat, and Representative Steve Scalise, a Louisiana Republican.

The proposed legislation “adds an extra layer of security that slams the door on Chinese actors from having a presence in the U.S. telecommunications network,” the lawmakers said in a news release.

Hikvision and Dahua have been accused by U.S. officials of involvement in China’s crackdown in far western Xinjiang, where as many as a million Uyghur Muslims have been placed in mass detention camps. China has repeatedly denied any accusations of human rights abuses against its Uyghur minority.

Still, the two companies remain leading suppliers of surveillance gear in the U.S., and together may sell about 1 million cameras this year, according to Conor Healy, government director for the surveillance research group IPVM.

“It’s still very widely sold to state and local governments” as well as school districts, Healy said in an interview. IPVM, based in Bethlehem, Pennsylvania, works to expose unethical surveillance. It draws its information from securities filings and purchasing records, Healy said.

School districts have been buying cameras in recent years in a bid to boost physical security following school shootings, said Keith Krueger, chief executive officer of CoSN, the Consortium for School Networking, an association for school technology officials.

Equipment from the targeted companies “is cheap and it’s good, and so people buy it,” said James Lewis, director of the strategic technologies program at the Center for Strategic & International Studies in Washington. “If you don’t know about the risk, it looks like a good deal.”

“If it’s connected over the internet and it goes back to China, you’d have no way to tell if the Chinese government was looking at it,” Lewis said.

Hikvision and Dahua account for about one-fifth of U.S. surveillance camera sales, placing each among the top 10 providers, said Jake Parker, senior director of government relations at the Security Industry Association, a trade group.

Parker called it “unprecedented” for the FCC to deny authorizations on grounds not related to technical details, or faults in applications.

The Consumer Technology Association told FCC officials the proposed changes “could be disruptive and impose substantial burdens on manufacturers well beyond the few covered entities,” according to a filing by the technology trade association.

Attachment 8

Hytera's Inclusion on FCC's National Security Blacklist 'Absurd,' Client Says

Diversified Communications Group said the FCC flubbed on adding Hytera to blacklist.



WASHINGTON, September 8, 2021 – A client of a company that has been included in a list of companies the Federal Communications Commission said pose threats to the security of the country's networks is asking the agency to reconsider including the company.

In a letter to the commission on Tuesday, Diversified Communications Group, which installs and distributes two-way radio communications devices to large companies, said the inclusion of Hytera Communications Corporation, a Chinese manufacturer of radio equipment, on a list of national security threats is "absurd" because the hardware involved is not connected to the internet and "does not transmit any sensitive or proprietary data."

"It seems that Hytera has been lumped in with other Chinese companies on the Covered List simply because they happen to manufacture electronics in the same country," Diversified's CEO **Ryan Holte** said in the letter, adding Hytera's products have helped Diversified's business thrive.

“This is a wrong that should be righted. Hytera is not a national security risk. They are an essential business partner to radio companies throughout the U.S.,” the CEO added.

In March, the FCC announced that it had [designated Hytera among other Chinese businesses](#) with alleged links to the Communist government. Others included Huawei, ZTE, Hangzhou Hikvision Digital Technology, and Dahua Technology.

[List among a number of restrictions on Chinese companies](#)

This list of companies was created in accordance with the Secure Networks Act, and the FCC indicated that it would continue to add companies to the list if they are deemed to “pose an unacceptable risk to national security or the security and safety of U.S. persons.”

Last month, the Senate commerce committee [passed through legislation](#) that would compel the FCC to no longer issue new equipment licenses to China-backed companies.

Last year the U.S. government took steps to ensure that federal agencies could not purchase goods or services from the aforementioned companies, and had previously added them to an economic blacklist.

In July, the FCC voted in favor of putting in place measures that would require U.S. carriers to [rip and replace](#) equipment by these alleged threat companies.

The Biden administration has been making moves to isolate alleged Chinese-linked threats to the country’s networks. In June, the White House [signed an executive order limiting investments](#) in predominantly Chinese companies that it said poses a threat to national security.

Attachment 9

September 14, 2021

VIA ELECTRONIC FILING (ECFS)

Acting Chairwoman Jessica Rosenworcel
Commissioner Brendan Carr
Commissioner Geoffrey Starks
Commissioner Nathan Simington
Federal Communications Commission
45 L Street NE
Washington, DC 20554

RE: *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program; Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program*
ET Docket No. 21-232, EA Docket No. 21-233

Dear Acting Chairwoman Rosenworcel and Commissioners:

We write as former FCC Acting General Counsel and former FCC Chief Counsel for Cybersecurity. While we advise numerous clients on these issues, we file this letter not on behalf of clients, but in our personal capacities as former public servants supportive of the FCC's valuable role in promoting the U.S. government's and the communications sector's efforts to ensure secure and reliable connectivity.

At the FCC, on Capitol Hill, at the Commerce Department, in interagency deliberations through the National Security Council, and now in private practice, we have participated substantially in every major cybersecurity and supply chain security effort that the U.S. government and the FCC have undertaken in the communications sector over the past four Presidential Administrations. Both within government and with private sector clients, we have helped develop and implement new regulatory and government-industry partnership frameworks, and we have a keen appreciation for the importance of proceeding carefully to ensure that, together, government and industry achieve the mutual benefits of security-related public policies.

We therefore urge the FCC to take action in this proceeding in close coordination with industry and interagency partners, and also with great care to avoid unintended practical and legal consequences. As we describe below, we recommend that the FCC: (1) base any prohibitions of future authorizations of "covered" equipment only on the Secure and Trusted

Communications Networks Act (“Secure Networks Act”)¹ and additional provisions in the pending Secure Equipment Act,² and (2) promote IoT security entirely outside the equipment authorization process through efforts coordinated with industry and federal partners.

I. The Secure Networks Act Directs the FCC to Identify “Covered” Communications Equipment That Poses Threats to U.S. National Security and to Prohibit Federal Subsidies for Such Equipment, and Congress Is Advancing Legislation Directing the FCC to Prohibit Such Equipment More Broadly.

We recognize the U.S. government’s national security interest in keeping “covered” equipment out of U.S. networks, first through the Secure and Trusted Communications Networks Reimbursement Program for Universal Service Fund (“USF”)-funded networks, and now, more generally, through the FCC’s equipment authorization process, which is required for all radio frequency (“RF”) devices marketed and operated in the country. We write to underscore that the process and the legal authority under which the FCC acts in this proceeding will set a new precedent for FCC action on behalf of the U.S. government, with potentially profound long-term ripple effects for supply chain security policy in general and the FCC’s equipment authorization process in particular.

A. The FCC’s National Security Authority to Exclude Covered Equipment Derives Solely from the Secure Networks Act, and This Authority Would Be Bolstered Further by Enactment of the Secure Equipment Act.

The FCC’s equipment authorization process is built upon the authority provided in Section 302 of the Communications Act to address harmful RF interference.³ As a practical matter, this process serves as a gating function for access to the U.S. marketplace and therefore provides a mechanism for the exclusion of covered equipment. However, the process is not based on, or authorized for, national security or cybersecurity functions, and we do not believe it is well-suited to being recast into performing such functions.

Therefore, we recommend that the FCC act to prohibit equipment authorizations for covered equipment only pursuant to the Secure Networks Act, with further explicit legal direction from the pending Secure Equipment Act. Such action would neither change the equipment authorization process nor rely on Section 302 authority; indeed, such action would not even “use” the equipment authorization process. Instead, ineligibility based on the Secure Networks Act would simply prohibit the process’s availability for designated covered equipment. Legally, this approach provides the FCC the strongest basis for action. Practically, it ensures that any future actions against subsequently designated covered equipment follow established, Congressionally-directed processes, without disrupting or complicating the equipment authorization process.

¹ Pub. L. No. 116-124, 134 Stat. 158, 170, codified at 47 U.S.C. §§ 1601-1609.

² Secure Equipment Act of 2021, S. 1790, 117th Cong. (2021). *See also* H.R. 3919, 117th Cong. (2021).

³ 47 U.S.C. § 302a.

The Secure Networks Act provides four direct statutory bases for specifically designating covered equipment that poses a threat to national security.⁴ In a separate provision, the Secure Networks Act also directs the FCC to bar designated entities from benefiting from subsidy programs administered by the FCC.⁵ In this proceeding, the NPRM proposes to establish a new administrative gating function that would deem covered equipment ineligible for the FCC's equipment authorization program. The Secure Networks Act is the only existing statute that provides appropriate authority for such an action. In contrast, proceeding pursuant to other legal authority – e.g., Section 302 – would be a questionable application and expansion of the FCC's authority, handing potential petitioners strong arguments for challenging the FCC's action.

In addition to this substantive recommendation, we offer a further recommendation regarding the sequencing of the FCC's action. Bipartisan leaders in both the House and the Senate are presently working to pass the Secure Equipment Act⁶ for the purpose of bolstering the FCC's authority to act in this proceeding.⁷ This pending legislation includes explicit authority to exclude covered equipment designated under the Secure Networks Act from the FCC's equipment authorization process, without amending the Commission's core equipment authorization mission to protect against harmful radio interference. This legislation has on-the-record support from Acting Chairwoman Rosenworcel and Commissioner Carr, and it has been unanimously reported out of the committees of jurisdiction in both the House and the Senate.⁸

⁴ 47 U.S.C. § 1601(c) (directing the Commission to base its determinations on one or more of the following determinations: (1) a specific determination made by any executive branch interagency body with appropriate national security expertise, including the Federal Acquisition Security Council established under section 1322(a) of title 41; (2) a specific determination made by the Department of Commerce pursuant to Executive Order No. 13873 (84 Fed. Reg. 22689, relating to securing the information and communications technology and services supply chain); (3) the communications equipment or service being covered telecommunications equipment or services, as defined in section 889(f)(3) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232, 132 Stat. 1918); and (4) a specific determination made by an appropriate national security agency).

⁵ 47 U.S.C. § 1602.

⁶ H.R. 3919 was considered by the House Committee on Energy and Commerce on July 21, 2021 and ordered to be reported as amended; S. 1790 was considered by the Senate Committee on Commerce, Science, and Transportation on August 4, 2021 and ordered to be reported with an amendment in the nature of a substitute.

⁷ See, e.g., H. Committee on Energy and Com., Subcomm. on Comm'n and Tech., Hearing on "A Safe Wireless Future: Securing our Networks and Supply Chains" (Jun. 30, 2021), available at <https://energycommerce.house.gov/committee-activity/hearings/hearing-on-a-safe-wireless-future-securing-our-networks-and-supply> (including an exchange between Rep. Steve Scalise and hearing witness Clete Johnson confirming Scalise's intent to bolster the FCC's legal standing through passage of the Secure Equipment Act).

⁸ See Press Release, Sen. Marco Rubio, "Rubio, Markey Applaud Commerce Committee Passage of Secure Equipment Act" (Aug. 4, 2021), available at

Given the forward momentum behind this legislation, we recommend that the FCC withhold final action on this proceeding until enactment of the Secure Equipment Act.

B. Revoking Previous Authorizations for Covered Equipment Would Be a Complex and Expensive Mandate with Uncertain and Potentially Marginal Benefits.

Absent enactment of a new statutory replacement and reimbursement regime, we recommend that the FCC not revoke previous authorizations. Legally and practically, revocation of previous authorizations would create significant problems that we believe would outweigh the potentially marginal security benefits of mandating and accelerating the unfunded removal of existing covered equipment.

Congress established a replacement and reimbursement regime in the USF context via the Secure Networks Act, but there are no analogous proposals pending before Congress to reimburse companies for replacing previously authorized covered equipment outside that USF context. To the contrary, the versions of the Secure Equipment Act that have been reported out of the committees of jurisdiction in the House and the Senate would prohibit the FCC from revoking previous authorizations under this proceeding.⁹

Companies large and small, as well as individual consumers, that presently use designated covered equipment that was authorized at the time of purchase will necessarily be transitioning away from future use as the equipment ages and newer alternatives enter the marketplace. Absent a funded program for replacement and reimbursement, the potential for revocation could raise extremely complex and disruptive challenges, including recalls and unfunded mandates to identify and replace equipment that in the future might be subject to revocation. This could reach well outside the communications sector and the national security arena. For instance, many convenience stores, self-storage facilities, schools, and other small entities use commodity surveillance cameras produced by covered entities that were authorized when purchased, and these cameras could conceivably be subject to revocation under this proceeding. Moreover, individuals with consumer electronics are likely to be, at best, confused, if they even become aware of any FCC revocation in the first instance.

Without a statutory replacement and reimbursement program, we think the public interest is best served by allowing for the necessary – and, for most companies, likely accelerated – attrition of previously authorized covered equipment.

<https://www.rubio.senate.gov/public/index.cfm/2021/8/rubio-markey-applaud-commerce-committee-passage-of-secure-equipment-act>.

⁹ While the versions of the Secure Equipment Act that were adopted by the committees of jurisdiction in the House and the Senate, respectively on July 21, 2021 and August 4, 2021, have not yet been published, it is our understanding that both versions contain a new provision that would prohibit the FCC from reviewing or revoking previous authorizations under the rules required by the legislation.

II. Ensuring the Efficiency of the FCC’s Equipment Authorization Process is Vital for U.S. Market Interests and for Meeting Connectivity Demands, and the FCC Should Not Base Its Efforts to Promote IoT Security on the Equipment Authorization Process.

As discussed above, we recommend that the FCC act to prohibit equipment authorizations for covered equipment only pursuant to the Secure Networks Act, with further explicit legal direction from the pending Secure Equipment Act, so as to avoid disruption to the current functioning or focus of the equipment authorization process. Similarly, we recommend that the FCC promote IoT security through initiatives that do not disrupt the equipment authorization process.

The FCC has developed its equipment authorization regime to implement Section 302’s authority to address harmful radio interference. The FCC leverages its limited engineering staff to great effect.¹⁰ The FCC Laboratory Division continuously provides general guidance (through the Office of Engineering and Technology’s Knowledge Database (“KDB”) publications) and specific guidance (through the KDB inquiry process) to the public in a timely manner. Any action in this proceeding that would change the fundamental nature of this process or add new substantive requirements unrelated to preventing RF interference could be highly disruptive and damaging to the process – and thus also to U.S. market interests and to efforts to meet the unprecedented connectivity demands of this era. Just two years ago, the 2018-19 government shutdown demonstrated the importance of a well-functioning equipment authorization process. Large product launches with the newest, most innovative equipment were jeopardized without access to the FCC’s engineers and its Equipment Authorization System.

As the FCC recognized in a recent Report and Order, the equipment authorization program is essential to ensuring that the devices Americans rely on every day comply with the FCC’s technical rules in an environment where increasing connectivity and accelerating product life cycles create increasing demand for authorizations.¹¹ We believe it is imperative that the equipment authorization process continue to meet the needs of U.S. businesses and consumers.

Accordingly, regarding the questions in the Notice of Inquiry, we recommend that the FCC seek to promote IoT security entirely outside the equipment authorization process. As a threshold matter, since general IoT security is distinct and separate as a legal and security issue from actions against designated covered equipment under the Secure Networks Act, any activities that the FCC undertakes to promote IoT security should occur separately from its actions under the NPRM and entirely outside the equipment authorization process. As noted above, this process is effective at addressing the risks associated with harmful radio interference, not cybersecurity.

¹⁰ As early as 2013, then-Commissioner Rosenworcel called for an Engineering Honors program to bolster the FCC’s engineering ranks. *See* Remarks of Commissioner Jessica Rosenworcel, IEEE GlobeCom 2013 (Dec. 11, 2013), at 5, <https://docs.fcc.gov/public/attachments/DOC-324651A1.pdf>.

¹¹ *Allowing Earlier Equipment Marketing and Importation Opportunities; Petition to Expand Marketing Opportunities for Innovative Technologies*, Report and Order, ET Docket No. 20-382 (2021).

Instead, FCC activities to promote IoT security should be closely coordinated with industry and government to promote private sector standards and certifications that are becoming powerful drivers of security in the global marketplace, as well as ongoing government-industry collaborative efforts to that same end (e.g., NISTIR 8259 and the consumer labeling pilot program led by NIST and the FTC under Executive Order 14028). For instance, given the Communications Security, Reliability, and Interoperability Council (“CSRIC”) VIII’s focus on 5G security, the FCC could direct CSRIC’s diverse experts to make recommendations to ensure that these standards and certifications continue to advance IoT security in 5G environments.

There are a number of such steps the FCC could take outside the equipment authorization process to put the FCC’s weight behind influential and concrete security advances that are supported by other federal partners and are already changing the global marketplace for secure IoT. In contrast, as a practical and legal matter, an attempt to use the FCC’s equipment authorization process to promote IoT security would divert resources from the critical core function of the FCC’s equipment authorization process, complicate the FCC’s contributions to IoT security, and potentially undermine the U.S. government’s broader efforts to advance IoT security. We think there is a better and more influential role for the FCC to play.

We commend you for your focus on these important issues. We stand ready to assist the Commission as this proceeding continues.

Sincerely,

/s/ Jennifer B. Tatel

Partner

Former FCC Acting General Counsel

/s/ Clete D. Johnson

Partner

Former FCC Chief Counsel for Cybersecurity